	Application No.	Applicant(s)
Notice of Allowability	09/277,335	KLEIN, DEAN A.
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/27/2005*.

2. ☒ The allowed claim(s) is/are *1,3-10,12-15,17 and 18*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All   b) ☐ Some*   c) ☐ None of the:

        1. ☐ Certified copies of the priority documents have been received.

        2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

        3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

        1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

    Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)

6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *03092006* .

7. ☒ Examiner's Amendment/Comment

8. ☐ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Eric Nelson on 3/9/2006. The application has been amended as follows:

PLEASE AMEND THE FOLLOWING CLAIMS AS FOLLOWS:

Claim 1 (currently amended):

In a personal computer having encryption hardware and a processor, a method of storing data on one or more magnetic or optical data storage media in an encrypted form comprising:

storing an identification code in a non-erasable memory during manufacture of the personal computer, wherein said identification code is defined at least in part by information associated with components of said personal computer;

retrieving the identification code from the non-erasable memory in said personal computer;

receiving user input;

generating a cryptographic key derived at least in part from said identification code and the received user input;

retrieving a checksum from a configuration register in a bus-to-bus bridge

in the personal computer, the bus-to-bus bridge storing information identifying

which of the <u>one or more magnetic or optical</u> data storage media is selected to

receive encrypted data;

verifying the generated cryptographic key, wherein verifying comprises

determining a checksum of the generated <u>cryptographic</u> key;

<u>retrieving information from a memory location;</u>

<u>disabling encryption of data routed to one of the one or more magnetic or</u>

<u>optical data storage media in response to said retrieved information;</u>

encrypting and decrypting data <u>based on the disabling step</u>, for storage on

and retrieval from one of <s>said</s> <u>the one or more magnetic or optical</u> data storage

media using <s>said</s> <u>the generated</u> cryptographic key, wherein the data is

transmitted by the processor and is encrypted in the personal computer by the

encryption hardware; <u>and</u>

<s>retrieving information from a memory location; and</s>

<s>disabling encryption of data routed to one of media in response to said</s>

<s>retrieved information.</s>

<u>storing the data in the one or more magnetic or optical data storage</u>

<u>media either in encrypted form or non-encrypted form based on the disabling</u>

<u>step.</u>

Claim 3 (currently amended):

The method of Claim 1, wherein said retrieving the identification code is performed without intervention by a host processor.

Claim 4 (currently amended):

The method of Claim 3, ~~additionally comprising verifying said key,~~ wherein said verifying occurs without intervention of said host processor.

Claim 5 (currently amended):

A method of making a computer comprising:

storing a hardware identifier in a non-erasable memory integrated circuit at the time of manufacture of ~~the~~ said computer, wherein the hardware identifier is defined at least in part by information associated with components of said computer, ~~the bus-to-bus bridge storing information identifying which data storage media is selected to receive encrypted data~~;

installing said non-erasable memory integrated circuit into said computer;

providing a data path to the data storage media;

providing a configuration register in a bus-to-bus bridge for storing a checksum, the bus-to-bus bridge storing information identifying which data storage media is selected to receive encrypted data;

coupling a logic circuit comprising an encryption engine to said data path; and

connecting said non-erasable memory integrated circuit to said logic circuit, wherein the hardware identifier and a user input is used by the encrypting engine for encrypting data that is transmitted to the data storage

media and for decrypting data that is retrieved from the data storage media, and

wherein the encryption engine verifies the generated cryptographic key using

the checksum, and wherein the encryption engine is configured to disable

encryption of data routed to the data storage media in response to information

retrieved from a storage location.

Claim 6 (currently amended):

The method of Claim 5, wherein said ~~act of~~ connecting comprises routing a

serial data bus from said <u>non-erasable</u> memory integrated circuit to said logic circuit.

Claim 7 (currently amended):

In a computer system comprising a processor and encryption hardware and at

least one data storage device, a method of data storage comprising:

        receiving user input;

        transmitting data from the processor in the computer system to <u>the</u>

encryption hardware in the computer system; and

        generating a cryptographic key derived at least in part from the received

user input and information that is stored in a non-erasable memory in said

computer system during manufacture of said computer system;

        retrieving a checksum from a configuration register in a bus-to-bus bridge

in ~~the~~ <u>said</u> computer system, the bus-to-bus bridge register storing information

identifying which storage device is selected to receive encrypted data;

        verifying the generated cryptographic key, wherein verifying comprises

determining a checksum of the generated key;

retrieving information from a memory location;

disabling encryption of data routed to said selected data storage device in

response to said retrieved information;

encrypting and decrypting, in the encryption hardware, user generated

data with an encryption process that uses the generated cryptographic key, the

encrypting and decrypting being based on the disabling step;

~~retrieving information from a memory location; and~~

~~disabling encryption of data routed to said data storage device in~~

~~response to said retrieved information.~~

storing the data in the at least one storage device either in encrypted

form or non-encrypted form based on the disabling step.

Claim 10 (currently amended):

The method of Claim 9, additionally comprising the act of deriving an

encryption key at least in part from said multi-bit identification code.

Claim 13 (currently amended):

The method of Claim 1, wherein encrypting data for storage is performed on an

encrypting device that is positioned in a data path between a central processing unit

and ~~the data storage medium~~ one of the one or more magnetic or optical data storage

media.

Claim 14 (currently amended):

The method of Claim 1, wherein all data that is transmitted to the <u>one or more</u> <u>magnetic or optical data storage</u> data storage media is encrypted.

Claim 15 (currently amended):

In a personal computer having encryption hardware and a processor, a method of storing data on one or more magnetic or optical data storage media in an encrypted form comprising:

storing an identification code in a non-erasable memory during manufacture of the personal computer, wherein said identification code is defined at least in part by information associated with components of said personal computer;

retrieving the identification code from the <u>non-erasable</u> memory in said personal computer;

receiving user input;

generating a cryptographic key derived at least in part from said identification code and the received user input;

retrieving a checksum from a configuration register in a bus-to-bus bridge circuit in ~~the~~ <u>said</u> personal computer, the bus-to-bus bridge circuit storing information identifying which of said <u>one or more magnetic or optical</u> storage media is selected to receive encrypted data;

verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key;

<u>retrieving information from a memory location;</u>

<u>disabling encryption of data routed to one of said storage media in</u>

<u>response to said retrieved information;</u>

encrypting and decrypting data based on the disabling step, for storage

on and retrieval from one of said <u>one or more magnetic or optical</u> data storage

media using said cryptographic key, wherein the data is transmitted by the

processor and is encrypted in the personal computer by the encryption

hardware, and wherein the encryption hardware is part of the bus-to-bus bridge

circuit; <u>and</u>

~~retrieving information from a memory location;~~

~~disabling encryption of data routed to one of said storage media in~~

~~response to said retrieved information.~~

<u>storing the data in the one or more magnetic or optical data storage</u>

<u>media either in encrypted form or non-encrypted form based on the disabling</u>

<u>step.</u>

Claim 17 (currently amended):

The method of Claim 15, wherein said retrieving <u>the identification code</u> is

performed without intervention by a host processor.

Claim 18 (currently amended):

The method of Claim 17, ~~additionally comprising verifying said key,~~ wherein

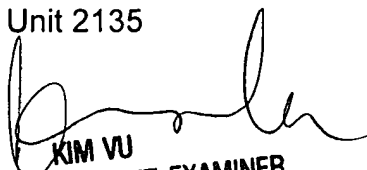said verifying occurs without intervention of said host processor.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100